What is claimed is:

1. A method for modifying validity of a certificate using biometric information in a public key infrastructure-based authentication system including a registration authority for verifying identity of at least one user by proxy, a certificate authority for issuing the identity-verified user with the certificate and a user system, the method comprising the steps of:

a) accessing a server of the certificate authority using login information of the user in response to a certificate validity modification request from the user under the condition that he/she is registered as a member in the authentication system;

b) inputting the biometric information for a user authentication through a biometric information input unit in the user system;

c) generating a certificate validity modification request message in response to the certificate validity modification request from the user; and

d) sending the inputted biometric information and the generated certificate validity modification request message to the certificate authority to request the certificate validity

modification online.

2. The method of claim 1, wherein the inputted biometric information and the generated certificate validity modification request message are encrypted with a public key of the certificate authority and sent thereto.

3. A method for modifying validity of a certificate using biometric information in a public key infrastructure-based authentication system including a registration authority for verifying identity of at least one user by proxy, a certificate authority for issuing the identity-verified user with the certificate and a user system, the method comprising the steps of:

a) receiving a message for requesting a certificate validity modification from the user system under the condition that the user system is connected to the authentication system via the Internet;

b) receiving login information and the biometric information entered from the user for a system member authentication if he/she requests the certificate validity modification;

c) determining whether the received biometric

information is the same as user's biometric information registered in a database storage unit if the user is authenticated on the basis of the received login information;

d) modifying the validity of the certificate issued to the user in response to the certificate validity modification request if the received biometric information is the same as the user's registered biometric information; and

e) sending to the user system an acknowledgment message for notifying the user that the certificate validity modification has been normally processed.

4. The method of claim 3, further comprising the step of:

a1) after performing the step a), checking integrity of the received certificate validity modification request message and sending to the user system an error occurrence message for notifying the user that the certificate validity modification has been not processed if there is an integrity compromise in the received certificate validity modification message.

5. The method of claim 3, further comprising the step of:

c1) sending to the user system an error occurrence message for notifying the user of a failure of member user authentication if it is determined at the step c) that the

received biometric information is not the same as the user's registered biometric information.

6. The method of claim 3, wherein the step d) includes the steps of:

d1) revoking the certificate issued to the user if the certificate validity modification request message indicates certificate revocation;

d2) suspending the certificate issued to the user if the certificate validity modification request message indicates certificate suspension; and

d3) recovering suspended authority of the certificate of the user if the certificate validity modification request message indicates certificate recovery.

7. The method of claim 3, wherein the database storage unit includes:

a user information database for storing user information under the condition that the user is registered as a member in the authentication system; and

a biometric information database for storing the biometric information of the user registered as a member, the user information and the biometric information being

registered and stored in such a way as to be matched with each other.

8. The method of claim 1 or claim 3, wherein the user system includes a biometric information input unit for inputting the biometric information of the user.

9. The method of claim 1 or claim 3, wherein the biometric information is information about a user's unique fingerprint.

10. The method of claim 1 or claim 3, wherein the biometric information is information about a user's unique iris.

11. The method of claim 1 or claim 3, wherein the biometric information is information about a user's unique face feature vector.